UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,344	07/22/2003	Jeffrey S. Bardsley	RSW920030077US1	7591

45832 7590 01/26/2011

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
01/26/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Patents@DillonYudell.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JEFFREY S. BARDSLEY, ASHLEY A. BROCK, CHARLES K. DAVIS III, NATHANIEL W. KIM, JOHN J. MCKENNA, and CARLOS F. VILLEGAS

Appeal 2009-005683
Application 10/624,344
Technology Center 2400

Before JOSEPH F. RUGGIERO, ROBERT E. NAPPI, and MARC S. HOFF, *Administrative Patent Judges.*

NAPPI, *Administrative Patent Judge.*

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

This is a decision on appeal under 35 U.S.C. § 134(a) of the rejection of claims 1 through 23.

We affirm.

INVENTION

The invention is directed to a method of generating security threat management information. See pages 4 and 5 of Appellants' Specification. Claim 1 is representative of the invention and is reproduced below:

1. A method of generating computer security threat management information, comprising:

receiving notification of a computer security threat;

generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and

transmitting the computer-actionable TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

REFERENCES

Gupta	US 2003/0004689 A1	Jan. 2, 2003
Friedrichs	US 2003/0084349 A1	May 1, 2003

REJECTIONS AT ISSUE

The Examiner has rejected claims 18 through 23 under 35 U.S.C. § 101 directed to non-statutory subject matter. The Examiner's rejection is on page 3 of the Answer.[2]

The Examiner has rejected claims 1 through 23 under 35 U.S.C. § 103(a) as being unpatentable Friedrichs in view of Gupta. The Examiner's rejection is on pages 3 through 9 of the Answer.

Rejection under 35 U.S.C. § 101

Appellants have not presented arguments directed to the Examiner's rejection under 35 U.S.C. § 101. Accordingly, *pro forma*, we sustain the Examiner's rejection of claims 18 through 23 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.[3]

ISSUES

Claims 1, 7 through 10, 16, and 17

Appellants argue on pages 6 through 9 of the Brief that the Examiner's rejection of claims 1, 7 through 10, 16, and 17 is in error. Appellants' arguments present us with three issues:

1) Did the Examiner err in finding that Friedrichs teaches a threat management vector having a field identifying at least one system that is affected by the security threat as claimed?

---

[2] Throughout this decision we refer to the Examiner's Answer dated December 27, 2007.
[3] Throughout this decision we refer to the Appeal Brief dated October 15, 2007 and the Reply Brief dated January 14, 2008.

2) Did the Examiner err in finding that Friedrichs teaches a threat management vector having a field identifying a release level for the system type affected as claimed?

3) Did the Examiner err in finding that Gupta teaches generating a threat management vector that is transmitted to a plurality of target systems as claimed?

Claims 2, 3, 4, 5, 6, and 11 through 23

Appellants present separate arguments directed to claim 2, 3, 4, 5, 6, and 11 through 23 which we address in the analysis section.

ANALYSIS

Claims 1, 7 through 10, 16 and 17

Appellants' arguments directed to the first two issues have not persuaded us of error in the Examiner's rejection. On pages 11 through 14 of the Answer, the Examiner responds to the Appellants' arguments by finding that Friedrichs teaches collecting data which include data identifying the system affected by the security threat and the release level as claimed. We concur with the Examiner's findings. Further, we are not persuaded by Appellants' arguments as they are directed to the information taught that is included in the threat management vector of Friedrichs being different than what is claimed. However, we note that claim 1 recites that this information is within a field (data field) but does not recite a function that operates using this data and, as such, the information in the fields is merely non-functional descriptive material. The Examiner need not give patentable weight to descriptive material absent a new and unobvious functional relationship between the descriptive material and the substrate. *See In re Lowry*, 32 F.3d 1579, 1583-84 (Fed. Cir. 1994); *In re Ngai*, 367 F.3d 1336, 1338 (Fed. Cir.

2004) and our recent final decision in *Ex parte Curry,* 2005-0509 (BPAI 2005), 84 USPQ2d 1272 (Affirmed, Rule 36, Fed. Cir., slip op. 06-1003, June 2006). Thus, even if the information in Friedrichs is different from the claimed data field, it would not distinguish Appellants' claim from the prior art.

Appellants' arguments directed to the third issue, whether the Examiner erred in finding that Gupta teaches generating a threat management vector that is transmitted to a plurality of target systems, have not persuaded us of that the rejection of claim 1 is in error. Appellants' arguments focus on the contention that Gupta's teaching of a file sent to sensor modules is not "computer actionable" as recited in claim 1. Brief 8, Reply Brief 4. The Examiner finds that Gupta teaches a file is transferred to the sensor systems which are part of the target systems. Answer 14-15. Further, the Examiner interprets the term "computer actionable" as including data that a computer acts on, by reading, writing, or changing. Answer 16. Based upon this claim interpretation, the Examiner finds that the attack file taught by Gupta is computer actionable. Answer 15-16. The Examiner also finds that Friedrichs in paragraphs 8, 25, and 33 teaches generating a report of threats to a processor for analysis, which also meets the claimed computer actionable threat management vector. Answer 16. We concur with the Examiner's claim interpretation as it is consistent with Appellants' Specification and the Examiner's findings regarding Gupta's attack file. Further, Appellants' argument on page 5 of the Reply Brief directed to this claim interpretation has not persuaded us that the Examiner's interpretation is inconsistent with the Specification. Thus, Appellants have not persuaded us that the Examiner erred in finding that Gupta teaches generating a threat management vector that is transmitted to a plurality of target systems.

As Appellants' arguments directed to the three issues have not persuaded us of error in the Examiner's rejection, we sustain the Examiner's rejection of claims 1, 7 through 10, 16, and 17.

Claim 2

Appellants argue on page 9 of the Brief that the Examiner erred in finding that Friedrichs teaches converting information from a database into computer-readable format. We are not persuaded by this argument since, as stated by the Examiner on page 18 of the Answer, claim 2 does not recite a limitation directed to converting data into a computer-readable format. Further, Appellants have not persuaded us that the Examiner erred in finding that Friedrichs teaches generating a threat management vector. As discussed above with respect to claim 1, we concur with the Examiner that Friedrichs teaches generating a threat management vector. Accordingly, we sustain the Examiner's rejection of claim 2.

Claim 3

Appellants argue on pages 9 and 10 of the Brief that the Examiner has not shown that Friedrichs teaches a "release level" as recited in claim 3. The Examiner responds on page 19 of the Answer that Friedrichs's teaching of a software version meets this limitation. We concur with the Examiner's finding and further note that the claimed "release level" is describing non-functional descriptive material and will not define the invention over the prior art. Accordingly, Appellants have not persuaded us of error and we sustain the Examiner's rejection of claim 3.

Claim 4

Appellants argue on page 10 of the Brief that the Examiner's rejection of claim 4 is in error as Friedrichs's disclosure may teach how to patch a flaw but does not teach that countermeasures are in a computer actionable format. The Examiner responds on pages 19 and 30 of the Answer that Friedrichs teaches security information is gathered and sent for analysis and, as such, is computer actionable (based upon the interpretation of this term discussed above with respect to claim 1). We concur with the Examiner's findings and note, as with claim 1, claim 4's discussion of countermeasures identifying a mode of installation is non-functional descriptive material, as it is merely identifying the type of data and not reciting performing a function with the data. Accordingly, Appellants have not persuaded us of error and we sustain the Examiner's rejection of claim 4.

Claim 5

Appellants argue on page 10 and 11 of the Brief that the Examiner has not shown that one of the indications in the third field of a computer actionable threat management vector comprises a pointer. Initially, we note that claim 5 does not recite that the pointer is in the third field and, as discussed with respect to claim 1, the data in the threat management vector is non-functional descriptive material as the claim does not recite performing any function with the data. Accordingly, Appellants have not persuaded us of error and we sustain the Examiner's rejection of claim 5.

Claim 6

Appellants argue on page 11 of the Brief that the Examiner has not explained how the Friedrich reference teaches the fourth and fifth computer

readable fields in the threat management vector as claimed. On pages 21 and 22 of Answer, the Examiner provides an explanation as to how Friedrichs teaches these fields. We concur with the Examiner's findings and further note that the description of the data in the fourth and fifth fields merely is non-functional descriptive material as the claim does not recite performing any function with the data. Accordingly, Appellants have not persuaded us of error and we sustain the Examiner's rejection of claim 6.

Claim 11

Appellants argues on pages 11 and 12 of the Brief, that the Examiner's rejection of claim 11 is in error as Friedrichs does not disclose making a threat management vector generator responsive to a semantics database. The Examiner finds that paragraph 45 of Friedrichs teaches a database, and that the discussion of claim 1 addresses the creation of a threat management vector. Answer 22. We concur with these findings and, as discussed with respect to claim 1, we concur with the Examiner's finding that Friedrichs teaches generating a report which meets the claimed threat management vector. Accordingly, Appellants' arguments have not persuaded of error and we sustain the Examiner's rejection of claim 11.

Claims 12 through 23

On pages 12 and 13 of the Brief, Appellants address these claims by merely identifying that the rejection should be reversed for the reasons given with respect to claims 2 through 6. As discussed above, Appellants' arguments directed to the rejection of claims 2 through 6 have not persuaded us of error. Accordingly, we sustain the Examiner's rejection of claims 12

through 23 under 35 U.S.C. § 103(a) for the reasons discussed above with respect to claims 2 through 6.

CONCLUSION

Appellants have not persuaded us of error in the Examiner's decision to reject claims 1 through 23.

ORDER

The decision of the Examiner to reject claims 1 through 23 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

ELD

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759